Mathematics

# MULTIPLE ATTACKS ON OVERSAMPLING OF FOURIER COEFFICIENTS METHOD FOR HIDING MESSAGES

Ghanshyam Bhatt[1], Lorraine Kraus[2], Laura Walters[3], Eric Weber[1]*
Iowa State University[1], Department of Mathematics, Ames, IA 50011; The College of New Jersey[2], Ewing, NJ 08628; Culver-Stockton College[3], Canton, MO 63435; esweber@iastate.edu

A system using an oversampled Fourier transform for hiding data is given in [J.R. Miotke and L. Rebollo-Neira, Applied Comp. Harmonic Anal., 16 (2004) no. 3, 203-207]. When viewed as a cryptographic algorithm, we demonstrate that the system is vulnerable to multiple types of attacks. This presentation would be of interest to both mathematicians and computer scientists.

L. Kraus and L. Walters were supported by NSF-REU grant No. DMS-0353880.
E. Weber was supported by NSF grant No. 0355573.